

ON A CLASS OF QUADRATIC POLYNOMIALS WITH NO ZEROS AND ITS APPLICATION TO APN FUNCTIONS

CARL BRACKEN, CHIK HOW TAN, AND YIN TAN

ABSTRACT. We show that there exists an infinite family of APN functions of the form $F(x) = x^{2^s+1} + x^{2^{k+s}+2^k} + cx^{2^{k+s}+1} + c^{2^k}x^{2^k+2^s} + \delta x^{2^k+1}$, over $\mathbb{F}_{2^{2k}}$, where k is an even integer and $\gcd(2k, s) = 1, 3 \nmid k$. This is actually a proposed APN family of Lilya Budaghyan and Claude Carlet who show in [6] that the function is APN when there exists c such that the polynomial $y^{2^s+1} + cy^{2^s} + c^{2^k}y + 1 = 0$ has no solutions in the field $\mathbb{F}_{2^{2k}}$. In [6] they demonstrate by computer that such elements c can be found over many fields, particularly when the degree of the field is not divisible by 3. We show that such c exists when k is even and $3 \nmid k$ (and demonstrate why the k odd case only re-describes an existing family of APN functions). The form of these coefficients is given so that we may write the infinite family of APN functions.

APN functions; zeros of polynomials; irreducible polynomials.

1. INTRODUCTION

Let \mathbb{F}_{2^n} be a finite field. The number of zeros of the polynomial

$$P_a(x) = x^{2^s+1} + x + a, \quad a \in \mathbb{F}_{2^n}^* \quad (1)$$

has been studied in [15, 16] as it has applications in several different contexts. For example, constructing difference sets with Singer parameters ([9, 10]), finding crosscorrelation between m -sequences ([13, 14]) and more recently in constructing error correcting codes [4]. Also, a similar problem concerning the polynomial $x^{p^s+1} + ax + b$ over \mathbb{F}_{p^n} has been considered by Bluher in [1], where p is an odd prime.

The following result, due to Helleseth and Kholosha ([15, Theorem 1]) shows that, when $\gcd(s, n) = 1$, the polynomial P_a can only have none, one or three zeros.

Result 1. *For any $a \in \mathbb{F}_{2^n}^*$ and a positive integer $l < n$ with $\gcd(l, n) = 1$, the polynomial $P_a(x) = x^{2^l+1} + x + a$ has either none, one, or three zeros in \mathbb{F}_{2^n} . Further, let M_i denotes the number of a such that $P_a(x)$ has i zeros, then*

(1) *If n is odd,*

$$M_0 = \frac{2^n+1}{3}, \quad M_1 = 2^{n-1} - 1, \quad M_3 = \frac{2^{k-1}-1}{3},$$

(2) *If n is even,*

$$M_0 = \frac{2^n-1}{3}, \quad M_1 = 2^{n-1}, \quad M_3 = \frac{2^{n-1}-2}{3}.$$

The condition that $P_a(x)$ has exactly one zero is also given in [15, Theorem 1]. In Section II, when n is even, we study the following problem.

For which $a \in \mathbb{F}_{2^n}^*$, does $P_a(x)$ have no zeros.

It is well known that $P_a(x)$ are related to other polynomials. More precisely, for a polynomial of the form $G(x) = x^{2^s+1} + \alpha x^{2^s} + \beta x + \gamma$ over \mathbb{F}_{2^n} , by letting $x = x + \alpha$, $G(x)$ can be reduced to the form $H(x) = x^{2^s+1} + \alpha x + \beta$. Moreover, by a simple substitution $x = sx$ with $s^{2^i} = \alpha$, $H(x)$ can be transformed into the form $P_a(x) = x^{2^s+1} + x + a$. Through the above transformations and the polynomials obtained in Theorem 1, we may get the ones with the forms G and H . These types of polynomials are of interest in other contexts.

Before getting into the application on APN functions, we would like to briefly introduce these functions. A function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is called *almost perfect nonlinear* (APN) if the number of solutions in \mathbb{F}_{2^n} of the equation

$$F(x + a) + F(x) = b$$

is at most 2, for all $a, b \in \mathbb{F}_{2^n}, a \neq 0$. We also say it has differential uniformity of 2. APN functions were introduced by Nyberg in [18], who defined them as the mappings with highest resistance to differential cryptanalysis. In other words, APN functions are those for which the plaintext difference $x - y$ yields the ciphertext difference $f(x) - f(y)$ with probability $1/2^{n-1}$. Since Nyberg's characterization, many new APN functions have been constructed, see [6, 2, 3, 7] and the references there. All the new infinite families (from 2005) have been quadratic (algebraic degree of 2) multinomials, as is the one in this article. When computing the differential uniformity of a quadratic function we may use the equation

$$F(x) + F(x + a) + F(a) = 0.$$

This is possible as the differential equation is linear.

Another application of APN functions is in the construction of error correcting codes. Each new APN function yields a new and inequivalent error correcting code with the parameters of the double error correcting BCH code. In fact, APN functions are said to be inequivalent if the extended BCH-like codes constructed from them are inequivalent codes, see [2] for details. We refer to inequivalent APN functions as CCZ-inequivalent (named after Carlet, Charpin and Zinoviev) [8]. This is a more general form of equivalence than the previously used affine and extended and affine equivalences. It is well known that CCZ equivalence preserves the differential and Walsh spectrum of the function. Some other equivalent descriptions of CCZ-equivalence and its invariants may be found in [12].

In [6], the authors construct a family of quadratic APN functions provided the existence of certain polynomials.

Result 2. *Let n and s be any positive integers, $n = 2k, \gcd(s, k) = 1$, and $c, s \in \mathbb{F}_{2^n}$ be such that $s \notin \mathbb{F}_{2^k}$. If the equation*

$$G(x) = x^{2^s+1} + cx^{2^s} + c^{2^k}x + 1 = 0$$

has no solution x such that $x^{2^k+1} = 1$, and in particular if the polynomial G is irreducible over \mathbb{F}_{2^n} , then the function

$$F_1(x) = x(x^{2^s} + cx^{2^k} + cx^{2^{k+s}}) + x^{2^s}(c^{2^k}x^{2^k} + sx^{2^{k+s}}) + x^{2^{k+s}+2^k}$$

is an APN function.

It was verified in [6] that the aforementioned irreducible polynomial G exist over many fields $\mathbb{F}_{2^{2k}}$ with $3 \nmid k$ by a computer. But, up to now, there is no construction of an infinite family of such polynomials. In Section III, when $n = 2k$ with k even and $3 \nmid k$, we construct the polynomials with the form $G(x)$ without zeros (Theorem 2) by applying the techniques used in Section II.

We will conclude this section by giving some remarks on the APN function F_1 in Result 2. Define the function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ by

$$F(x) = x^{2^s+1} + x^{2^{k+s}+2^k} + cx^{2^{k+s}+1} + c^{2^k}x^{2^k+2^s} + \delta x^{2^k+1},$$

where $n = 2k, \delta \notin \mathbb{F}_{2^k}$. One may check that, if $n = 2k$ with k odd, F is CCZ-equivalent to the multinomial APN function in [2, Theorem 1] by substituting x with $x + \gamma x^{2^k}$. Also, if k is even, F is CCZ-equivalent to F_1 in Result 2 by substituting x with $x + \gamma x^{2^k+2^s}$, where γ is not a $(2^k - 1)$ -th power. Therefore, to prove the existence of the APN function F_1 in Result 2, it is sufficient to consider the case k is even and the existence of F . One reason

here to consider the function F instead of the hexanomial one F_1 is that F is equivalent to the No. 4 function in the list of quadratic APN functions over fields with dimension 8 in Dillon's paper [11], and the No. 4 function is also a 5-term polynomial. It should be mentioned that we know the family of APN functions we are constructing are inequivalent to other families, as computer evidence has verified that it is not equivalent to any power mapping when $n = 8$ [6]. Also for $n = 8$ we have checked by computer that F is not equivalent to $x^3 + \text{Tr}(x^9)$. F has Γ -rank 13200 (see the definition in [12]), while $x^3 + \text{Tr}(x^9)$ has Γ -rank 13800. Furthermore, it must be different from the other recently discovered non power mapping APN functions as its defined on fields with different degrees. In fact, it is a distinguishing factor of the family under consideration here that it can be defined on fields with degrees that are powers of 2. This property is seen as desirable by some (and necessary by others) in cryptographic applications. The only other APN functions with this property are the power mappings x^{2^s+1} and $x^{2^{2s}-2^s+1}$, known as the Gold and Kasami functions as well as $x^3 + \text{Tr}(x^9)$. These three functions are defined on fields with any degree.

2. A TYPE OF QUADRATIC POLYNOMIALS WITH NO ZEROS

In this section, we will study for which $a \in \mathbb{F}_{2^n}^*$, the polynomial $P_a(x) = x^{2^s+1} + x + a$ has no zeros, where $n = 2k$ and $\gcd(2k, s) = 1$.

Theorem 1. *Let $P_a(x) = x^{2^s+1} + x + a$ over $\mathbb{F}_{2^{2k}}$, with $(2k, s) = 1$. Then P_a has no zeros if there exists a non-cube $b \in \mathbb{F}_{2^{2k}}$ such that*

$$a = A(b) = \frac{b(b+1)^{2^s+2^{-s}}}{(b+b^{2^{-s}})^{2^s+1}}.$$

Proof. We start with the following polynomial,

$$K(x) = b \left(x + \frac{b^{2^{-s}} + 1}{b + b^{2^{-s}}} \right)^{2^s+1} + \left(x + \frac{b^{2^{-s}+1} + b}{b + b^{2^{-s}}} \right)^{2^s+1}.$$

Note that $b + b^{2^{-s}}$ is always not zero as b is neither 1 nor 0. We will demonstrate that K has no zeros by setting $K(x) = 0$, which gives

$$b \left(x + \frac{b^{2^{-s}} + 1}{b + b^{2^{-s}}} \right)^{2^s+1} = \left(x + \frac{b^{2^{-s}+1} + b}{b + b^{2^{-s}}} \right)^{2^s+1}.$$

As one side of this expression is a cube, while the other is not, the only possible solutions are when its identically zero. This implies

$$x = \frac{b^{2^{-s}} + 1}{b + b^{2^{-s}}} = \frac{b^{2^{-s}+1} + b}{b + b^{2^{-s}}},$$

which in turn implies that $b = 1$, which it's not.

Next, we expand $K(x) = 0$ and gather terms to obtain,

$$\begin{aligned} (b+1)x^{2^s+1} + \left(b \left(\frac{b^{2^{-s}} + 1}{b + b^{2^{-s}}} \right) + \frac{b^{2^{-s}+1} + b}{b + b^{2^{-s}}} \right) x^{2^s} + \left(b \left(\frac{b+1}{b + b^{2^s}} \right) + \frac{b^{2^s+1} + b^{2^s}}{b + b^{2^s}} \right) x \\ + b \left(\frac{b^{2^{-s}} + 1}{b + b^{2^{-s}}} \right)^{2^s+1} + \left(\frac{b^{2^{-s}+1} + b}{b + b^{2^{-s}}} \right)^{2^s+1} = 0. \end{aligned}$$

This becomes

$$(b+1)x^{2^s+1} + (b+1)x + \frac{b(b+1)^{2^s+2^{-s}+1}}{(b+b^{2^{-s}})^{2^s+1}} = 0.$$

Now, we divide by $b+1$ and with a few simplifications we obtain,

$$P_a(x) = x^{2^s+1} + x + \frac{b(b+1)^{2^s+2^{-s}}}{(b+b^{2^{-s}})^{2^s+1}} = 0.$$

So $P_a(x) = 0$ can not have solutions in $\mathbb{F}_{2^{2k}}$ and hence $P_a(x)$ has no zeros when a has the required form. \square

Particularly, when $s = 1$, we may show that $P_a(x)$ has no zeros if and only if a is with the form in Theorem 1. Furthermore we may claim the polynomial is irreducible as it has degree 3.

Corollary 1. *The polynomial $P_a(x) = x^3 + x + a$ is irreducible over $\mathbb{F}_{2^{2k}}$, for any integer k , if and only if $a = d + d^{-1}$ for some non-cube d .*

Proof. Substituting $s = 1$ in $A(b)$, we have

$$\begin{aligned} A(b) &= \frac{b(b+1)^{2+2^{-1}}}{(b+b^{2^{-1}})^{2+1}} \\ &= \frac{b(b^{2^{-1}}+1)^{2 \cdot (2+2^{-1})}}{b^{3 \cdot 2^{-1}}(b^{2^{-1}}+1)^3} \\ &= \frac{b+1}{b^{2^{-1}}}. \end{aligned}$$

By Theorem 1, if $a = A(b) = \frac{b+1}{b^{2^{-1}}}$, then $P_a(x)$ has no zeros. For a simpler form we let $b = d^2$ and a has the form $d + d^{-1}$ for a non cube d . Conversely, by Result 1, there are $\frac{2^n-1}{3}$ elements a such that P_a has no zeros. Therefore, we only need to prove that $|\text{Im}(A)| = \frac{2^n-1}{3}$. Letting C denote the set of non cubes in $\mathbb{F}_{2^{2k}}$, it can be easily verified that $A(x) = A(x^{-1})$ for any $x \in C$ and $|C| = \frac{2(2^n-1)}{3}$, so it is sufficient to prove that A is 2-to-1. Assume there exist $x, y \in C$ such that $A(x) = A(y)$, after simplification, we get $xy(x+y) = x+y$. Since $x, y \neq 0$, we have $x = y$ or $xy = 1$. This shows that A is 2-to-1 and the proof is finished. \square

Using a computer, for small values of n , we found the size of the image set of A is $(2^n - 1)/3$. This implies that, in Theorem 1, P_a has no zeros if and only if $a \in \text{Im}(A)$. However, we cannot prove this and leave this as a conjecture.

Conjecture 1. *Let $n = 2k$ with k is even and C be the set of non-cubes. Define a function $A : C \rightarrow \mathbb{F}_{2^n}$ by*

$$A(b) = \frac{b(b+1)^{2^s+2^{-s}}}{(b+b^{2^{-s}})^{2^s+1}}.$$

The polynomial $P_a(x) = x^{2^s+1} + x + a$ has no zeros if and only if $a \in \text{Im}(A)$.

Remark 1. *We outline a possible method for solving this problem. It can be easily verified that $A(b) = A(b^{-1})$ and since $|C| = \frac{2(2^n-1)}{3}$, it will be sufficient to prove A is a 2-to-1 mapping.*

By Theorem 1 and the relationship between the polynomials of the form $G(x) = x^{2^s+1} + \alpha x^{2^s} + \beta x + \gamma$ and $P_a(x) = x^{2^s+1} + x + a$ mentioned in Section I, we may obtain polynomials with no zeros of the form G . In the next section, we will use a variation of the method used in Theorem 1 to find the polynomial with no zeros and with the form $x^{2^s+1} + cx^{2^s} + c^{2^k}x + 1$ over $\mathbb{F}_{2^{2k}}$ with k is even, for some $c \in \mathbb{F}_{2^{2k}}$. It is the existence of this polynomial that guarantees the existence of the infinite family of APN functions. We will show that for all relevant fields a coefficient c exists such that the polynomial has no zero's.

3. A FAMILY OF 5-TERM APN FUNCTIONS

Through the rest of the paper, we assume k is an even integer and $3 \nmid k$. In this section, we will show that the function

$$F(x) = x^{2^s+1} + x^{2^{k+s}+2^k} + cx^{2^{k+s}+1} + c^{2^k}x^{2^k+2^s} + \delta x^{2^k+1}$$

is an APN function over $\mathbb{F}_{2^{2k}}$ by choosing a particular type of $c, \delta \in \mathbb{F}_{2^{2k}}$. The nature of the coefficients was difficult to find and we require the following lemma to show that they exist.

Lemma 1. *Let $\mathbb{L} = \mathbb{F}_{2^{2k}}$ and k, s be integers such that $(s, 2k) = 1$ with k is even and $3 \nmid k$. Then there exist $\beta, \gamma \in \mathbb{L}^*$ such that*

$$\gamma^{2^s+1} + \omega\beta^{2^s+1} + 1 = 0, \quad (2)$$

where ω has order 3 in \mathbb{L} and $\gamma^{2^k-1} \neq \beta^{2^k-1}$.

Proof. Let \mathbb{L}^3 denotes the set of cubes in \mathbb{L} . First, note that all non-cubes in \mathbb{L} can be written as $\omega c, \omega^2 c$ for some $c \in \mathbb{L}^3$. We claim that there exist $a, b, c \in \mathbb{L}^3$ such that

$$a + b = \omega c. \quad (3)$$

If this was not the case then the set of cubes would form an additive, as well as a multiplicative, group and hence yield a subfield of \mathbb{L} with an impermissible number of elements.

Let D denotes the elements of $\mathbb{F}_{2^{2k}}$ which are not in \mathbb{F}_{2^k} . Now we consider the possible cubes that satisfy (3) with respect to whether they are in the subfield \mathbb{F}_{2^k} or in its complement D . If all solutions to (3) are such that a, b and c are always in D then the cubes in \mathbb{F}_{2^k} would form an additive group and yield another impossible subfield. On the other hand if all solutions are such that a, b and c are always contained in the subfield \mathbb{F}_{2^k} , then the set of cubes in D would form a group under addition with $\frac{2^{2k}-2^k}{3}$ elements. But this is not a power of 2 and is therefore impossible. We conclude from the above arguments that there exists a solution a, b, c to (3) with at least one element in \mathbb{F}_{2^k} and another in D .

We divide (3) by a to obtain,

$$1 + \frac{b}{a} + \omega \frac{c}{a} = 0.$$

Letting α be primitive in \mathbb{L} and assuming that $b/a = \alpha^t, \omega c/a = \alpha^r$, we rewrite the above equation as,

$$1 + \alpha^t + \alpha^r = 0. \quad (4)$$

All we can say about t and r is that $3 \mid t$ while $3 \nmid r$ and that at least one of α^t and α^r is not in \mathbb{F}_{2^k} .

From Equation (4) we will give two constructions of the required equation

$$\gamma^{2^s+1} + \omega\beta^{2^s+1} + 1 = 0,$$

and show that at least one of them has to allow the condition $\gamma^{2^k-1} \neq \beta^{2^k-1}$.

Construction 1: We construct β and γ as follows. Let $\alpha^t = \gamma^{2^s+1}$ and $\alpha^r = \omega\beta^{2^s+1}$. The existence of β, γ is guaranteed by the fact that $(s, 2k) = 1$ and then $(2^s + 1, 2^{2k} - 1) = 3$, so all cubes can be represented as $(2^s + 1)$ -th powers. This gives the required equation (2). Next we will assume that $\gamma^{2^k-1} = \beta^{2^k-1}$.

Therefore,

$$\gamma^{(2^s+1)(2^k-1)} = \beta^{(2^s+1)(2^k-1)}.$$

We now write this equation in terms of the primitive element α and obtain,

$$\alpha^{t(2^k-1)} = (\omega^2\alpha^r)^{2^k-1}.$$

As $\omega^3 = 1$ and $2^k - 1$ is divisible by 3, a rearrangement yields

$$\alpha^{(t-r)(2^k-1)} = 1.$$

Because α is primitive we know that $(t-r)(2^k-1) \equiv 0 \pmod{2^{2k}-1}$. This implies that $t = r$ or $\alpha^{t-r} \in \mathbb{F}_{2^k}$. The $t = r$ case is easily dismissed as t and r are not equivalent mod 3. The other case we save for later.

Construction 2: We construct β and γ differently from above. We start with (4). Next, we divide by α^t to obtain,

$$\alpha^{-t} + 1 + \alpha^{r-t} = 0.$$

Now, we let $\alpha^{-t} = \gamma^{2^s+1}$ and $\alpha^{r-t} = \omega\beta^{2^s+1}$. Again, we get our required Equation (2). Now assume that

$$\gamma^{2^k-1} = \beta^{2^k-1},$$

which implies,

$$\gamma^{(2^s+1)(2^k-1)} = \beta^{(2^s+1)(2^k-1)}.$$

As before we write this in terms of α and get

$$\alpha^{-t(2^k-1)} = (\omega^2\alpha^{r-t})^{2^k-1}.$$

This yields

$$\alpha^{r(2^k-1)} = 1.$$

Note that the β and γ are different in this construction but the α is the same α as in Construction 1.

In this case $r = 0$ or $\alpha^r \in \mathbb{F}_{2^k}$. It is clear that $r \neq 0$. But if α^r is in \mathbb{F}_{2^k} then this construction hasn't worked. Just like if α^{t-r} is in \mathbb{F}_{2^k} , then the first construction hasn't worked. But we only require one of them to work so when we assume $\alpha^r \in \mathbb{F}_{2^k}$ and $\alpha^{t-r} \in \mathbb{F}_{2^k}$ together we get $\alpha^r \in \mathbb{F}_{2^k}$ and $\alpha^t \in \mathbb{F}_{2^k}$ which contradicts an earlier claim and the proof is complete. \square

Next we will use the β and γ in Lemma 1 and a modification of the techniques in Theorem 1 to prove the existence of the following family of APN functions.

Theorem 2. *Let s and k be integers, with k even, such that $(s, 2k) = 1$ and $3 \nmid k$. We choose $\delta \notin \mathbb{F}_{2^k}$, ω to have order 3 and β and γ such that $\gamma^{2^s+1} + \omega\beta^{2^s+1} + 1 = 0$ with $\gamma^{2^k-1} \neq \beta^{2^k-1}$. Then the function*

$$F(x) = x^{2^s+1} + x^{2^{k+s}+2^k} + (\omega\beta^{2^s+2^k} + \gamma^{2^s+2^k})x^{2^{k+s}+1} + (\omega\beta^{2^{k+s}+1} + \gamma^{2^{k+s}+1})x^{2^k+2^s} + \delta x^{2^k+1}$$

is an APN function on $\mathbb{F}_{2^{2k}}$.

Proof. The existence of the coefficients is guaranteed from Lemma 1. To prove the function is APN we need to show that the equation

$$F(x) + F(x + a) + F(a) = 0$$

has no more than 2 solutions for all nonzero $a \in \mathbb{F}_{2^{2k}}$. Placing $F(x)$ into this equation and then replacing x with ax will give

$$\begin{aligned} & a^{2^s+1}(x + x^{2^s}) + a^{2^{k+s}+2^k}(x^{2^{k+s}} + x^{2^k}) + a^{2^{k+s}+1}(\omega\beta^{2^s+2^k} + \gamma^{2^s+2^k})(x + x^{2^{k+s}}) \\ & + a^{2^k+2^s}(\omega\beta^{2^{k+s}+1} + \gamma^{2^{k+s}+1})(x^{2^k} + x^{2^s}) + a^{2^k+1}\delta(x + x^{2^k}) = 0. \end{aligned} \quad (5)$$

We raise this equation to the 2^k -th power and obtain a second equation,

$$\begin{aligned} & a^{2^{k+s}+2^k}(x^{2^{k+s}} + x^{2^k}) + a^{2^s+1}(x + x^{2^s}) + a^{2^k+2^s}(\omega\beta^{2^{k+s}+1} + \gamma^{2^{k+s}+1})(x^{2^k} + x^{2^s}) \\ & + a^{2^{k+s}+1}(\omega\beta^{2^s+2^k} + \gamma^{2^s+2^k})(x + x^{2^{k+s}}) + a^{2^k+1}\delta^{2^k}(x + x^{2^k}) = 0. \end{aligned}$$

When we add these two expressions together, we simply get

$$a^{2^k+1}(\delta + \delta^{2^k})(x + x^{2^k}) = 0.$$

As $a \neq 0$ and $\delta \notin \mathbb{F}_{2^k}$ this implies that $x \in \mathbb{F}_{2^k}$. Then our original equation (5) becomes

$$(a^{2^s+1} + a^{2^{k+s}+2^k} + a^{2^{k+s}+1}(\omega\beta^{2^s+2^k} + \gamma^{2^s+2^k}) + a^{2^k+2^s}(\omega\beta^{2^{k+s}+1} + \gamma^{2^{k+s}+1}))(x + x^{2^s}) = 0$$

Clearly this will permit only 2 solutions in x provided we can establish that

$$a^{2^s+1} + a^{2^{k+s}+2^k} + a^{2^{k+s}+1}(\omega\beta^{2^s+2^k} + \gamma^{2^s+2^k}) + a^{2^k+2^s}(\omega\beta^{2^{k+s}+1} + \gamma^{2^{k+s}+1}) \neq 0,$$

for all non zero a . To this end we divide by a^{2^s+1} and let $y = a^{2^k-1}$, which gives the following,

$$G(y) = y^{2^s+1} + (\omega\beta^{2^s+2^k} + \gamma^{2^s+2^k})y^{2^s} + (\omega\beta^{2^{k+s}+1} + \gamma^{2^{k+s}+1})y + 1$$

which if it has no zeros, proves $F(x)$ is APN. To show that $G(y)$ has no zeros, we will set it equal to zero and use the techniques in Theorem 1 to produce a factoring which allows no solutions. The β and γ were chosen very carefully to allow the usage of this technique.

From $\omega^2\beta^{-2^s-1}G(y) = 0$, we obtain

$$\omega^2\beta^{-2^s-1}y^{2^s+1} + (\beta^{2^k-1} + \omega^2\gamma^{2^s+2^k}\beta^{-2^s-1})y^{2^s} + (\beta^{2^{k+s}-2^s} + \omega^2\gamma^{2^{k+s}+2^s}\beta^{-2^s-1})y + \omega^2\beta^{-2^s-1} = 0.$$

A simple rearrangement of $\gamma^{2^s+1} + \omega\beta^{2^s+1} + 1 = 0$ will allow us to write the coefficient of y^{2^s+1} as $\omega^2(\frac{\gamma}{\beta})^{2^s+1} + 1$. The coefficient of y^{2^s} can be rewritten as

$$\omega^2(\frac{\gamma}{\beta})^{2^s+1}\gamma^{2^k-1} + \beta^{2^k-1},$$

while the coefficient of y can be written as

$$\omega^2 \left(\frac{\gamma}{\beta}\right)^{2^s+1} \gamma^{2^{k+s}-2^s} + \beta^{2^{k+s}-2^s}.$$

Now, using the fact that,

$$\gamma^{2^k(2^s+1)} + \omega\beta^{2^k(2^s+1)} = 1,$$

we can alter the last term, $\omega^2\beta^{-2^s-1}$, as follows,

$$\begin{aligned} \omega^2\beta^{-2^s-1} &= \omega^2\beta^{-2^s-1}(\gamma^{2^k(2^s+1)} + \omega\beta^{2^k(2^s+1)}) \\ &= \omega^2\left(\frac{\gamma}{\beta}\right)^{2^s+1}\gamma^{(2^s+1)(2^k-1)} + \beta^{(2^s+1)(2^k-1)}. \end{aligned}$$

Placing these alternate forms of the coefficients into $\omega^2\beta^{-2^s-1}G(y) = 0$ yields,

$$\begin{aligned} (\omega^2\left(\frac{\gamma}{\beta}\right)^{2^s+1} + 1)y^{2^s+1} + (\omega^2\left(\frac{\gamma}{\beta}\right)^{2^s+1}\gamma^{2^k-1} + \beta^{2^k-1})y^{2^s} + (\omega^2\left(\frac{\gamma}{\beta}\right)^{2^s+1}\gamma^{2^{k+s}-2^s} + \beta^{2^{k+s}-2^s})y \\ + \omega^2\left(\frac{\gamma}{\beta}\right)^{2^s+1}\gamma^{(2^s+1)(2^k-1)} + \beta^{(2^s+1)(2^k-1)} = 0. \end{aligned}$$

This implies

$$\begin{aligned} \omega^2\left(\frac{\gamma}{\beta}\right)^{2^s+1}(y^{2^s+1} + \gamma^{2^k-1}y^{2^s} + \gamma^{2^s(2^k-1)}y + \gamma^{(2^s+1)(2^k-1)}) \\ = y^{2^s+1} + \beta^{2^k-1}y^{2^s} + \beta^{2^s(2^k-1)}y + \beta^{(2^s+1)(2^k-1)}. \end{aligned}$$

Next we factor each side to obtain,

$$\omega^2\left(\frac{\gamma}{\beta}\right)^{2^s+1}(y + \gamma^{2^k-1})^{2^s+1} = (y + \beta^{2^k-1})^{2^s+1}.$$

Clearly the right hand side of this expression is a cube while the left hand side is not. So the only possible solutions occur when $y = \gamma^{2^k-1} = \beta^{2^k-1}$, but as we have chosen γ and β such that $\gamma^{2^k-1} \neq \beta^{2^k-1}$, we can now say that $G(y)$ has no zeros and the proof is complete. \square

We cannot determine the Fourier (Walsh) spectrum of the APN function F in Theorem 2 and we leave this as an open problem. By a computer (with $n = 8$), the Fourier spectrum of F is the same as the Gold APN functions, i.e., the spectrum should takes the values $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$.

All other known APN functions have had their Fourier spectra computed, see [5] and references therein. This is done for two reasons. The first is a cryptographic application. Knowing a functions spectrum can allow us to compute its nonlinearity, which measures the functions resistance to Matsui's linear attack [17]. Secondly, the weight distribution of the codewords in the BCH-like code constructed from the function is also determined by the functions spectrum. All codes derived from an APN function will have a minimum distance of 5, but the weight distributions differ among some of the six power mapping APN functions. The infinite families of multi-term quadratic APN functions discovered since 2005 all have the same spectrum as the gold function and we expect the function in this article to be no different.

Conjecture 2. *The Fourier spectrum of the APN function F in Theorem 2 is $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$.*

4. CONCLUSIONS

In this paper, we considered the polynomial $P_a(x) = x^{2^s+1} + x + a$ over \mathbb{F}_{2^n} with $\gcd(n, s) = 1$. It is shown that if $a = \frac{b(b+1)^{2^s+2^{-s}}}{(b+b^{2^{-s}})^{2^s+1}}$ for some non-cube b , then $P_a(x) = 0$ has no solutions. Moreover, we conjecture that the converse of this result is also true. In particular, we show that $x^3 + x + a$ is irreducible if and only if $a = d + d^{-1}$, for some non cube d . By applying the techniques used here we obtain an infinite family of polynomials with no zero's of the form $x^{2^s+1} + cx^{2^s} + c^{2^k}x + 1$ over $\mathbb{F}_{2^{2k}}$ with k even and $\gcd(2k, s) = 1, 3 \nmid k$. This guarantees the existence of the infinite family of quadratic APN functions proposed by Budaghyan and Carlet in [6].

ACKNOWLEDGEMENT

We would like to thank Dr. Longjiang Qu for careful reading of this manuscript and many helpful discussions.

REFERENCES

- [1] A. W. Bluhner, On $x^{q+1} + ax + b$, Finite Fields Appl. 10 (3), 285–305, 2004.
- [2] C. Bracken, E. Byrne, N. Markin, and G. McGuire, New families of quadratic almost perfect nonlinear trinomials and multinomials, Finite Fields Appl. 14, 703–714, 2008.
- [3] C. Bracken, E. Byrne, N. Markin and G. McGuire, A few more quadratic APN functions, Cryptography and Communications 3 (1), 43–53, 2011.
- [4] C. Bracken, T. Helleseht, Triple-error-correcting BCH-like codes, IEEE International Symposium on information theory, 1723–1725, 2009
- [5] C. Bracken, Zhengbang Zha, On the Fourier spectra of the infinite families of quadratic APN functions, Advances in Mathematics of Communications, 3(3), 219–226, 2009.
- [6] L. Budaghyan and C. Carlet, Classes of quadratic APN trinomials and hexanomials and related structures, IEEE Trans. Inform. Theory 54 (5), 2354–2357, 2008.
- [7] L. Budaghyan, C. Carlet and G. Leander, Two classes of quadratic APN binomials inequivalent to power functions. IEEE Trans. Inform. Theory 54, no. 9, 4218–4229, 2008.
- [8] C. Carlet, P. Charpin, V. Zinoviev, Bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography 15(2), 125–156, 1998.
- [9] J. F. Dillon, Geometry, codes and difference sets: Exceptional connections, in: A. Seress, K. T. Arasu (Eds.), Codes and Designs, in: Ohio State Uni. Math. Res. Inst. Publ., vol. 10, de Gruyter, Berlin, 73–85, 2002.
- [10] J. F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields Appl. 10 (3), 342–389, 2004.
- [11] J. F. Dillon, Almost perfect nonlinear polynomials: An update. In: 9th International Conference on Finite Fields and Applications of Fq9, Dublin, Ireland, 2009.
- [12] Y. Edel, A. Pott, A new almost perfect nonlinear function which is not quadratic, Adv. Math. Commun. 3, no. 1, 59–81, 2009.
- [13] H. Dobbertin, P. Felke, T. Helleseht, P. Rosendahl, Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums, IEEE Trans. Inform. Theory 52 (2), 613–627, 2006.
- [14] T. Helleseht, A. Kholosha, G.J. Ness, Characterization of m -sequences of lengths $2^{2k} - 1$ and $2^k - 1$ with three-valued crosscorrelation, IEEE Trans. Inform. Theory 53 (6), 2236–2245, 2007.
- [15] T. Helleseht and A. Kholosha, On the equation $x^{2^i+1} + x + a = 0$ over $GF(2^k)$, Finite Fields Appl. 14, 159–176, 2008.
- [16] T. Helleseht and A. Kholosha, $x^{2^i+1} + x + a$ and related affine polynomials over $GF(2^k)$, Cryptogr. Commun. 2, 85–109, 2010.
- [17] M. Matsui, Linear cryptanalysis method for DES cipher, EUROCRYPT, 55–64, 1993.
- [18] K. Nyberg Differentially uniform mappings for cryptography, Advances in Cryptology-EUROCRYPT 93, LNCS 765, 55–64, 1994.

DEPARTMENT OF MATHEMATICS, SCHOOL OF PHYSICAL & MATHEMATICAL SCIENCES, NANYANG TECHNOLOGY UNIVERSITY, SINGAPORE.

E-mail address: `carlbracken@ntu.edu.sg`

TEMASEK LABORATORIES, NATIONAL UNIVERSITY OF SINGAPORE, 117411 SINGAPORE

E-mail address: `tsltch@nus.edu.sg`

TEMASEK LABORATORIES, NATIONAL UNIVERSITY OF SINGAPORE, 117411 SINGAPORE

E-mail address: `itanyinmath@gmail.com`